We claim:

1. A method for implementing secure communication, comprising:

(a) receiving instructions to initiate a process for creating a secure communication link to a remote device via a publicly accessible network;

(b) determining, in response to the instructions received in step (a), whether at least one local application program used to create the secure communication link is configured;

(c) initiating, based on the instructions received in step (a), a second process for accessing a database over the publicly accessible network;

(d) receiving, in response to step (c) and if the at least one local application program is not configured, configuration information for the at least one program;

(e) configuring the at least one program based upon the configuration information received in step (d); and

(f) creating the secure communication link based on the configuration.

2. The method of claim 1, wherein:

the secure communication link is a VPN connection, and

the information received in step (d) comprises at least one of a public/private key pair and a certificate.

3. The method of claim 1, further comprising:

(g) determining whether an update to the at least one application program is available;

(h) receiving the update; and

(i) implementing the update.

4. The method of claim 1, wherein:

the secure communication link is a VPN connection,

step (b) comprises determining if a client certificate is present,

step (c) comprises, if a client certificate is not present, requesting enrollment of a client certificate, and

step (d) comprises receiving a client certificate.

5. The method of claim 1, wherein step (d) comprises receiving a generic VPN policy without PKI data, and further comprising:

(g) generating PKI data and a corresponding certificate enrollment request;

(h) sending the certificate enrollment request to the remote device for forwarding to an external certification authority (CA); and

(i) receiving a certificate.

6. The method of claim 4, wherein the received client certificate is enrolled, in cooperation with an internal corporate certification authority, with an external certification authority.

7. The method of claim 1, wherein step (c) comprises initiating an automatic content update (ACU) application.

8. The method of claim 7, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and further comprising:

(g) determining whether an update is available for at least one of the additional application programs; and

(h) receiving an update for the at least one additional application program.

9. The method of claim 7, wherein the ACU application communicates with the remote device and other remote device on behalf other application programs.

10. The method of claim 7, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and further comprising:

(g) fetching from the remote device content or content metadata applicable to at least one of the additional application programs; and

(h) storing, by the at least one additional application program, the fetched content or content metadata.

11. The method of claim 7, wherein the ACU application communicates using a SyncML protocol.

12. The method of claim 7, further comprising:

(g) storing, in a configuration record for at least one application, an Internet Access Point (IAP) to be used when communicating with a remote device on behalf of the at least one application.

13. The method of claim 7, wherein the ACU application communicates using a simple request-response protocol, and wherein a protocol transaction consists of a single request-response pair.

14. The method of claim 7, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and further comprising:

(g) fetching from the remote device content metadata applicable to at least one of the additional application programs;

(h) comparing fetched metadata to locally stored metadata; and

(i) fetching new or updated content from the remote device based upon the comparison.

15. The method of claim 14, wherein the ACU application includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the remote device.

16. The method of claim 7, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and further comprising:

(g) fetching, from multiple databases in the remote device, metadata about multiple types of content.

17. The method of claim 7, wherein

the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and

the ACU application transmits requests containing properties used by the remote device to filter requests.

18. The method of claim 7, wherein messages generated by the ACU application and communicated to the remote device include a message identifier, a target database identifier, and a security level.

19. The method of claim 18, wherein a first security level is required to receive configuration information for the at least one program and a second security level is required to receive another type of information.

20. The method of claim 18, wherein at least one message generated by the ACU application includes an element indicating that a message is the last message relating to a specific task.

21. The method of claim 18, wherein the ACU application requests configuration information in a single message.

22. The method of claim 7 further comprising, upon receipt of a first response from the remote device:

(g) validating and storing a returned certificate to create a trust relationship with the remote device.

23. The method of claim 22, further comprising:

(h) using the returned certificate to validate subsequent responses from the remote device.

24. The method of claim 23, wherein:

the returned certificate is validated based on a hash calculated over the entire ACU message resulting in the first response from the remote device, except for a signature element of the ACU message,

the hash is signed with a private key held by the remote device, and

the corresponding certificate is included in the first response and is used by the recipient to verify the signature and identify and authenticate the sender.

25. A device for secure communication with a server via a publicly accessible network, comprising:

an interface to a publicly accessible network; and

a processor configured to perform steps comprising:

(a) receiving instructions to initiate a process for creating a secure communication link to a remote device via a publicly accessible network;

(b) determining, in response to the instructions received in step (a), whether at least one local application program used to create the secure communication link is configured;

(c) initiating, based on the instructions received in step (a), a second process for accessing a database over the publicly accessible network;

(d) receiving, in response to step (c) and if the at least one local application program is not configured, configuration information for the at least one program;

(e) configuring the at least one program based upon the configuration information received in step (d); and

(f) creating the secure communication link based on the configuration.

26. The device of claim 25, wherein:

the secure communication link is a VPN connection, and

the information received in step (d) comprises at least one of a public/private key pair and a certificate.

27. The device of claim 25, wherein the processor is further configured to perform steps comprising:

(g) determining whether an update to the at least one application program is available;

(h) receiving the update; and

(i) implementing the update.

28. The device of claim 25, wherein:

the secure communication link is a VPN connection,

step (b) comprises determining if a client certificate is present,

step (c) comprises, if a client certificate is not present, requesting enrollment of a client certificate, and

step (d) comprises receiving a client certificate.

29. The device of claim 1, wherein step (d) comprises receiving a generic VPN policy without PKI data, and wherein the processor is further configured to perform steps comprising:

(g) generating PKI data and a corresponding certificate enrollment request;

(h) sending the certificate enrollment request to the remote device for forwarding to an external certification authority (CA); and

(i) receiving a certificate.

30. The device of claim 28, wherein the received client certificate is enrolled, in cooperation with an internal corporate certification authority, with an external certification authority.

31. The device of claim 25, wherein step (c) comprises initiating an automatic content update (ACU) application.

32. The device of claim 31, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and wherein the processor is further configured to perform steps comprising:

(g) determining whether an update is available for at least one of the additional application programs; and

(h) receiving an update for the at least one additional application program.

33. The device of claim 31, wherein the ACU application communicates with the remote device and other remote device on behalf other application programs.

34. The device of claim 31, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and wherein the processor is further configured to perform steps comprising:

(g) fetching from the remote device content or content metadata applicable to at least one of the additional application programs; and

(h) storing, by the at least one additional application program, the fetched content or content metadata.

35. The device of claim 31, wherein the ACU application communicates using a SyncML protocol.

36. The device of claim 31, wherein the processor is further configured to perform steps comprising:

(g) storing, in a configuration record for at least one application, an Internet Access Point (IAP) to be used when communicating with a remote device on behalf of the at least one application.

37. The device of claim 31, wherein the ACU application communicates using a simple request-response protocol, and wherein a protocol transaction consists of a single request-response pair.

38. The device of claim 31, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and wherein the processor is further configured to perform steps comprising:

(g) fetching from the remote device content metadata applicable to at least one of the additional application programs;

(h) comparing fetched metadata to locally stored metadata; and

(i) fetching new or updated content from the remote device based upon the comparison.

39. The device of claim 38, wherein the ACU application includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the remote device.

40. The device of claim 7, wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and wherein the processor is further configured to perform steps comprising:

(g) fetching, from multiple databases in the remote device, metadata about multiple types of content.

41. The device of claim 31, wherein

the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and

the ACU application transmits requests containing properties used by the remote device to filter requests.

42. The device of claim 31, wherein messages generated by the ACU application and communicated to the remote device include a message identifier, a target database identifier, and a security level.

43. The device of claim 42, wherein a first security level is required to receive configuration information for the at least one program and a second security level is required to receive another type of information.

44. The device of claim 42, wherein at least one message generated by the ACU application includes an element indicating that a message is the last message relating to a specific task.

45. The device of claim 42, wherein the ACU application requests configuration information in a single message.

46. The device of claim 31, wherein the processor is further configured to perform steps comprising, upon receipt of a first response from the remote device:

(g) validating and storing a returned certificate to create a trust relationship with the remote device.

47. The device of claim 46, wherein the processor is further configured to perform steps comprising:

(h) using the returned certificate to validate subsequent responses from the remote device.

48. A server, comprising:

an interface to a publicly accessible network; and

a processor configured to perform steps comprising:

(a) receiving requests from multiple users for configuration information for locally stored application programs used to create secure communication links to the server, the users being organized in a hierarchy of child, parent and grandparent groups, each group having a corresponding set of secure communication configuration data accessible by the server, each child group inheriting properties from its parent group, each parent group inheriting properties its grandparent group;

(b) storing content associated with the groups, with information associated with a particular group being accessible to the particular group and to groups inheriting properties from the particular group;

(b) providing configuration information to the users, the configuration information provided to each user comprising the configuration data set for each group from which the user inherits properties;

(c) receiving requests from the users for content corresponding to other locally stored application programs; and

(d) providing information to the users of a child group based on the groups from which the child group inherits properties.